REMARKS

Claims 1-3, 5-11, 14-16, and 18-28 are currently pending in the subject application and are presently under consideration. Claims 1, 3, 5-7, 9, 11, 15-16, 18, 19, 22, and 26-28 have been amended as shown on pages 3-10 of the Reply. In addition, the specification has been amended as indicated on page 2.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-5, 9, 10, 12-21, 26, and 27 Under 35 U.S.C. §103(a)

Claims 1-5, 9, 10, 12-21, 26, and 27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Stallings (Cryptography and Network Security; Third Edition, Chapter 9 / Public-Key Cryptography: 9.1: Principles of Public-Key Cryptosystems, Upper Saddle River, NJ Prentice Hall, 2003, pgs. 250-265, 290-293, 444, and 655) in view of Bentley, *et al.* (US 2003/0217275). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Stallings and Bentley, *et al.*, individually or in combination, do not disclose all aspects set forth in the subject claims.

> To reject claims in an application under § 103, an examiner must establish a prima facie case of obviousness. A prima facie case of obviousness is established by a showing of three basic criteria. First, there must be some apparent reason to combine the known elements in the fashion claimed by the patent at issue (*e.g.*, in the references themselves, interrelated teachings of multiple patents, the effects of demands known to the design community or present in the marketplace, or in the knowledge generally available to one of ordinary skill in the art). To facilitate review, this analysis should be made explicit. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. See MPEP § 706.02(j). See also KSR Int'l Co. v. Teleflex, Inc., 550 U.S. ____, 04-1350, slip op. at 14 (2007). The reasonable expectation of success must be found in the prior art and not based on applicant's disclosure. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)

The subject claims relate to the use of session keys to facilitate secure message exchange during a dialog between two systems. The session key can be generated when a dialog session is initiated between an initiator of the dialog and a target of the dialog. The session key can subsequently encrypted at the initiator system and transmitted to the target system to be used by the respective systems for encryption and decryption of messages during the dialog. Encryption of the session key can be performed using both the private key of the dialog initiator as well as a public key associated with the target system. When a dialog is initiated to access a service on a remote system, the particular public key used to encrypt the session key for such a session can be determined according to a remote service binding that defines a binding between the service and a particular public key (or a digital certificate having an associated public key). In particular, amended independent claim 1 recites, *a binding component that creates a remote service binding between a user's digital certificate and a remote service associated with a target system, the remote service binding specifying that the user's digital certificate is to be used when a dialog is initiated between the initiator system and the remote service*.

Stallings does not disclose these aspects. Stallings provides an overview of public-key encryption systems, whereby communicating parties encrypt messages using shared public keys of respective public-private key pairs. However, Stallings does not contemplate *binding a particular public key with a remote service running on a system*, such that initiating a dialog with the remote service causes the specified public key to be used to encrypt a session key for the dialog. Rather, Stallings teaches that selection of a public key is strictly a function of the party with which communication is desired. That is, when communicating with a selected destination party, the destination party's public key is used for encryption. The cited reference does not disclose that the public key used for encryption during a dialog with a remote service can be determined according to a *prearranged binding between the remote service and a selected public key*.

Bentley, *et al.* is also silent regarding these aspects. Bentley, *et al.* relates to a method of controlling access to a file using digital signatures. A file's author determines what access rights a selected user is to be granted with respect to a file to be protected, encrypts these rights with a master password, stores the encrypted rights as well as an encrypted version of the password with the file, and performs an additional encryption of the file using the password. However, Bentley, *et al.* does not disclose a remote service binding that *associates a service with a particular public key*, such that initiating a dialog to this service causes the bound public key to be used to encrypt a session key for the dialog. Like Stallings, Bentley, *et al.* teaches that the public key used for encryption of a file is a function of the intended recipient, but does not contemplate binding a particular public key *with a remote service* using a remote service binding.

The claimed subject matter also discloses that, once a dialog has been initiated and a session key for the dialog has been generated, the session key can be twice-encrypted prior to sending the key to the target system. That is, the session key can first be encrypted using a private key associated with the initiator of the dialog, and the result of this encryption can be further encrypted using the public key associated with the remote service at the target in accordance with the aforementioned remote service binding. The result of these encryptions can then be sent to the target to facilitate secure message exchange during the dialog. To this end, amended independent claim 1 goes on to recite, *a session key generator that generates a session key for a dialog between the initiator system and the remote system at the target system, the session key employed to securely exchange a message associated with the dialog; and, an encryption component that employs asymmetric encryption to* ***encrypt the session key using a private key associated with the initiator system to yield a first session key encryption, encrypt the first session key encryption using the public key specified by the remote service binding to yield an encrypted session key output****, and securely transmit the encrypted session key output to the target system, the session key thereafter being employed to encrypt the message and securely exchange the message between the initiator system and the target system.* As already discussed, neither Stallings nor Bentley, *et al.* discloses a remote service binding that specifies a public key to be used for encryption when a dialog to a given service is initiated. The cited references also fail to disclose subsequently using this bound public key to encrypt a session key for the dialog after the session key has already been encrypted by the private key of the initiator. While Stallings discloses that a message can be encrypted using both a sender's private key and the recipient's public key, as noted in the Office Action dated February 23, 2009, the cited reference teaches that the public key selected for this encryption is dependent exclusively on the intended recipient of the message. The cited reference does not contemplate that a public key for this type of encryption can be selected in accordance with a *previously created remote service binding* that defines which public key will be used for dialogs with a particular service.

With regard to decryption, amended independent claim 14 recites, *a session key employed to securely exchange a message associated with a dialog between an initiator system and a remote service running on a target system,* ***the session key twice encrypted using a private key***

associated with the initiator system and a public key specified according to a remote service binding that associates the public key with the remote service running on the target system; *and, a decryption component that receives the encrypted version of the session key from the initiator system, employs asymmetric decryption to decrypt the encrypted session key using a private key associated with the target system to yield a first session key decryption, and decrypts the first session key decryption using a public key associated with the initiator system to yield the session key, the session key thereafter being employed to decrypt a received encoded version of the message*. As discussed *supra*, neither cited reference discloses a remote service binding as recited in amended independent claim 14.

Similarly, amended independent claim 18 recites, ***establishing a remote service binding at a first system that binds a service running on a second system with a particular user's digital certificate***; *initiating a dialog at the first system with the service running on the second system; identifying the digital certificate bound to the service upon initiating the dialog; firstly encrypting a symmetric session key with a private key associated with an initiator of the dialog to yield a first encryption;* ***secondly encrypting a result of the first encryption with a public key associated with the identified digital certificate to yield a second encryption.*** Stallings and Bentley, *et al.* do not contemplate encrypting a session key according to a remote service binding that links a remote service with a particular public key, as already noted.

Also, amended independent claim 26 recites, *a first data field comprising a remote service binding that* ***associates a service running on a remote system with a particular user's public key***; *and a data field comprising an encrypted session key,* ***the session key encrypted using a private key associated with an initiator of a message to the service and the public key associated with the service by the remote service binding***. As discussed above, neither cited reference discloses or suggests encrypting a session key for a message exchange using a public key selected according to a *remote service binding* that associates the key with a remote service.

Likewise, amended independent claim 27 recites, *means for* ***creating a remote service binding that associates a service running on a first system with a particular public key***; *means for initiating a message exchange between the first system and a second system, the message exchange involving access to the service running on the first system; means for receiving an encrypted session key from the second system*, ***the encrypted session key encrypted using a private key associated with the second system and the public key associated with the service by***

the remote service binding. Stallings and Bentley, *et al.* are silent regarding these aspects, as noted *supra*.

Providing additional detail regarding creation of a remote service binding, amended claim 5 recites, *the remote service binding created at the initiator system using the following syntax:*

> *Create Remote Service Binding <LOGICAL SERVICE NAME>*
> *To Service '<SERVICE>'*
> *With (User = [<USER>])*

where <LOGICAL SERVICE NAME> is a logical name assigned to the service by the binding, <SERVICE> is the remote service, and <USER> is an identification of the user whose public key is to be utilized when a dialog is initiated with the remote service by the initiator system. As already discussed, Stallings and Bentley, *et al.* fail to disclose or suggest creation of a remote service binding as previously described. The cited references therefore also fail to disclose that such a binding can be created at the system initiating the dialog using the syntax recited in amended claim 5.

In view of at least the foregoing, it is respectfully submitted that Stallings and Bentley, *et al.*, individually or in combination, do not disclose or suggest all features set forth in amended independent claims 1, 14, 18, and 26 (and all claims depending there from), and as such fail to make obvious the present invention. It is therefore requested that this rejection be withdrawn.

II. Rejection of Claim 11 Under 35 U.S.C. §103(a)

Claim 11 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Stallings (Cryptography and Network Security; Third Edition, Chapter 9 / Public-Key Cryptography: 9.1: Principles of Public-Key Cryptosystems, Upper Saddle River, NJ Prentice Hall, 2003, pgs. 250-265, 290-293, 444, and 655) and Bentley, *et al.* (US 2003/0217275). However, claim 11 depends from amended independent claim 1, and as discussed in the previous section of the Reply in connection with that independent claim, neither of the cited references disclose or suggest binding a particular public key with a remote service running on a system, such that initiating a dialog with the remote service causes the specified public key to be used to encrypt a session key for the dialog. It is therefore respectfully submitted that this rejection should be withdrawn with respect to amended claim 11.

III. Rejection of Claims 6-8 Under 35 U.S.C. §103(a)

Claims 6-8 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Stallings (Cryptography and Network Security; Third Edition, Chapter 9 / Public-Key Cryptography: 9.1: Principles of Public-Key Cryptosystems, Upper Saddle River, NJ Prentice Hall, 2003, pgs. 250-265, 290-293, 444, and 655) and Bentley, *et al.* (US 2003/0217275) in view of VanHeyningen, *et al.* (US 2002/0112152). However, claims 6-8 depend from amended independent claim 1, and as already discussed, neither Stallings nor Bentley, *et al.* disclose the remote service binding functionality set forth in that independent claim. VanHeyningen, *et al.* also fails to disclose these aspects. VanHeyningen, *et al.* relates to a technique for delivering encrypted data to a client *via* proxy servers that perform processing on the data prior to delivery to a client. This processing allows each individual data record to be decrypted independently of previously received data records. However, VanHeyningen, *et al.* nowhere discloses binding a public key to a service using a remote service binding, and encrypting a session key to be used for a message exchange session with the service using a public key selected in accordance with this binding.

In view of at least the foregoing, it is respectfully submitted that Stallings, Bentley, *et al.*, and VanHeyningen, *et al.*, individually or in combination, do not disclose all aspects of amended independent claims 1 and 22 (and all claims depending there from), and as such fail to make obvious the present invention. It is therefore requested that this rejection be withdrawn.

IV. Rejection of Claim 28 Under 35 U.S.C. §103(a)

Claim 28 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Stallings (Cryptography and Network Security; Third Edition, Chapter 9 / Public-Key Cryptography: 9.1: Principles of Public-Key Cryptosystems, Upper Saddle River, NJ Prentice Hall, 2003, pgs. 250-265, 290-293, 444, and 655) and Bentley, *et al.* (US 2003/0217275) in view of Wasilewski, *et al.* (US 5,870,474). However, amended claim 28 depends from amended independent claim 1, and as discussed *supra*, neither Stallings nor Bentley, *et al.* disclose or suggest a remote service binding that associates a public key with a service, and causes the associated public key to be used for encryption of a session key when a dialog is established to that service, as set forth in that independent claim. Wasilewski, *et al.* is also silent regarding these features. Wasilewski, *et al.* relates to delivery of multi-media data from a service provider to an end user. According to Wasilewski, *et al.*, the multimedia data packets are first encrypted using random number generated keys, which themselves are encrypted using a second randomly generated key. This second key is itself encrypted using a public key associated with a set top unit to which the data is to be delivered. As can be seen, none of these encryptions utilize a key that has been *associated with a particular service via a remote service binding*. Rather, the cited system employs keys that are either randomly generated or are associated with the particular client to which the data is to be delivered. Consequently, Wasilewski, *et al.* fails to remedy the deficiencies of Stallings and Bentley, *et al.* in this regard. It is therefore respectfully submitted that this rejection should be withdrawn.

V. Rejection of Claims 22-25 Under 35 U.S.C. §103(a)

Claims 22-25 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Stallings (Cryptography and Network Security; Third Edition, Chapter 9 / Public-Key Cryptography: 9.1: Principles of Public-Key Cryptosystems, Upper Saddle River, NJ Prentice Hall, 2003, pgs. 250-265, 290-293, 444, and 655), Bentley, *et al.* (US 2003/0217275), and VanHeyningen, *et al.* (US 2002/0112152) in view of Wasilewski, *et al.* (US 5,870,474). However, amended independent claim 22 recites, *establishing a dialog between a dialog initiator and a service running on a target system; receiving at the target system an encrypted session key from the dialog initiator,* ***the encrypted session key encrypted using a private key associated with the dialog initiator and a public key specified by a remote service binding that associates the public key with the service running on the target system***. As discussed *supra*, none of the cited references disclose such a remote service binding. It is therefore respectfully requested that this rejection be withdrawn with respect to amended independent claim 22 (and claims 23-25, which depend there from).

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP566US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,
TUROCY & WATSON, LLP

/Brian Steed/
Brian Steed
Reg. No. 64,095

TUROCY & WATSON, LLP
127 Public Square
57TH Floor, Key Tower
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731